

HiPER CLI 配置手册

——业务管理

版权声明

版权所有©2000-2004，上海艾泰科技有限公司，保留所有权利。

本文档所提供的资料包括 URL 及其他 Internet Web 站点参考在内的所有信息，如有变更，恕不另行通知。

除非另有注明，本文档中所描述的公司、组织、个人及事件的事例均属虚构，与真实的公司、组织、个人及事件无任何关系。

本手册及软件产品受最终用户许可协议（EULA）中所描述的条款和条件约束，该协议位于产品文档资料及软件产品的联机文档资料中，使用本产品，表明您已经阅读并接受了 EULA 中的相关条款。

遵守所生效的版权法是用户的责任。在未经艾泰科技有限公司明确书面许可的情况下，不得对本文档的任何部分进行复制、将其保存于或引进检索系统；不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。艾泰科技有限公司拥有本文档所涉及主题的专利、专利申请、商标、商标申请、版权及其他知识产权。在未经艾泰科技有限公司明确书面许可的情况下，使用本文档资料并不表示您有使用有关专利、商标、版权或其他知识产权的特许。

艾泰®、UTT®文字及相关图形是艾泰科技有限公司的注册商标。

HiPER®文字及其相关图形是上海艾泰科技有限公司的注册商标。

此处所涉及的其它公司、组织或个人的产品、商标、专利，除非特别声明，归各自所有人所有。

产品编号（PN）：0900-0028-001

文档编号（DN）：PR-PMMU-1106.01-PPR-CN-1.0A

目　录

导　　读

命令行格式约定

本手册中，命令行格式约定的描述如下：

粗体：命令行关键字采用加粗字体表示，指配置命令时需要原封不动输入的部分。

斜体：命令行参数采用斜体表示，指配置命令时必须由实际值进行替代的部分。

[ ]：表示用[ ]扩起来的部分，在配置命令时是可选的。

{x | y | … }：表示从两个或多个选项中选取一个。

[x | y | …]：表示从两个或多个选项中选取一个或者不选。

//：由//开始的行表示注释行

注意：

1. 本手册中，通常情况下，命令行参数不区分大小写，以下除外：
    a） 登录时的用户名和密码，
    b） 用户使用删除自定义的策略（Filter 或时间段）时，删除（delete）命令中的策略名与新建该策略时自定义的策略名必须大小写严格匹配。举例如下：

        // 新建一个 filter 策略，策略名为 TEST（以大写方式输入）
        new filter in/TEST
        // 删除策略 TEST（必须以大写方式输入）
        delete filter in/TEST

2. 本手册的所有配置实例中，均是 HiPER 的 LAN 口接到内网，WAN 口接到 Internet；同时，在 HiPER 的 LAN 口启用 Filter，过滤从局域网内部到 Internet 的流量。

1 业务管理功能介绍

Internet 发展的同时也带来了一些副作用，如出现了赌博、色情等和国家法律法规相悖的网站；宽带网络给大众提供快速冲浪的同时，网络蠕虫病毒也得到快速传播，给电脑使用者带来很大的威胁。各个机构需要连接到 Internet，因此也制定了具体的上网规则，如某些地方规定公务员不能在上班时间炒股和通过即时消息聊天，企业不允许电脑使用者操作和工作无关的事情，家长需要能在指定的控制孩子的上网时间，蠕虫病毒和黑客攻击充斥网络，需要将它们挡在攻击电脑之前等，不一而足。

我们可以把整个网络分成三个层次，一个是核心层，接下来是汇聚层，和用户最接近的是接入层。因为管理的多样性，在接入层实施控制是理想的选择。一方面，可以根据各个机构的具体特点发展本机构特色的业务，另外一个方面，将大量的控制分散到接入层，对于汇聚和核心两个层次也是起到了分解压力的作用。

HiPER 系列的业务管理功能正是为解决这些问题而开发。

灵活地运用 HiPER 的业务管理功能，不仅能够为不同的用户设置不同的 Internet 访问权限，还可以控制用户在不同时段的 Internet 访问权限。在实际应用中，可根据各个机构的管理规则，然后制定出相应的业务管理策略，在 HiPER 上实施。如在学校使用 HiPER 作为宽带接入设备时，可设置学生不能访问游戏网站；而对于家庭来说，只在指定的时间内允许孩子上网；企业的财务部门的机器不能被互联网访问，对于各种攻击包括病毒的过滤等。

HiPER 的业务管理功能是根据用户定义的策略，监测流经 HiPER 的每个包，结合 HiPER 的防火墙技术 Filter 来实现的。Filter 的机制就是分析流经 HiPER 的数据包，针对数据包的特点，如源地址、目标地址、上层协议或其他信息，通过定义一些策略对经过路由器（网关）接口上的数据包进行控制：转发或丢弃。

对于 HiPER 而言，包有进入和外出两个方向。HiPER 系列产品所能处理的包可以是进入 HiPER，或者从 HiPER 往外出，对这些包的动作可以是转发，或者是丢弃。包的类型可以是基本的 IP 包，这个是基本的包过滤防火墙的功能，也可以是扩展的功能，如 Ethernet 包，还可以根据时间段来实施包的过滤动作。HiPER 还有一个特别之处，还可以根据数据包的内容的值来过滤。

1.1 Filter 类型

HiPER 可提供三种基本的 Filter 类型：IP Filter，IPSSG Filter 和 Generic Filter。

1.1.1 IP Filter 介绍

IP Filter 只是对 IP 包进行判断和处理，其过滤依据主要是 IP 包头部信息，如源地址和目的地址。如果 IP 头中的协议字段封装协议为 TCP 或 UDP，则再根据 TCP 头信息（源端口和目的端口）或 UDP 头信息（源端口和目的端口）执行过滤。

1.1.2 IPSSG Filter 介绍

IPSSG Filter 是扩展的 Filter，是 HiPER 专有的 Filter。IPSSG Filter 的过滤依据除了 IP Filter 中的所有过滤依据之外，还包括 MAC 地址、时间段等信息。另外，IPSSG Filter 还支持分组功能，可以通过 GROUPNAME 来设置不同的规则集合（组），当需要多个控制策略用在不同的地方时，可以使用 IPSSG 的分组功能。

1.1.3 Generic Filter 介绍

Generic Filter 是按照字节（bytes）或者比特（bits）检查任意类型的数据包。使用 Generic Filter，管理员需要知道所需要匹配包的某些字节的具体内容，比如说，某几个字节表示协议，那么就可以匹配相应协议的包。

1.1.4 三种类型比较

上述三种类型中，Generic Filter 执行效率最高，IP Filter 执行效率其次，IPSSG Filter 的效率最低。

IPSSG Filter 是在 IP Filter 基础上的扩充：IP Filter 具备的功能，IPSSG Filter 均具备。但是 IPSSG Filter 支持 MAC 地址过滤、时间段过滤，IP Filter 不支持。因此，考虑到执行效率，当需要配置的 Filter 策略不涉及到 MAC 地址、时间段信息时，建议使用 IP Filter。当然，如果需要过滤 MAC 地址或时间段，则只能使用 IPSSG Filter。

Generic 主要用于 IP 协议之外的访问控制，如对使用 IPX、NETBIOS 等协议的控制；还可用于对应用程序的控制，如 QQ、MSN 等。

需要注意的是，HiPER 系列产品均支持 IP Filter 和 Generic Filter。业务管理系列产品均支持 IPSSG 功能，请查看相关产品的规格说明书。另外，还可使用 revision 命令查看，如果输出结果" Feature enabled "中包含 IPSSG 功能，则表示该产品可以使用 IPSSG Filter，下面给出一个例子。

```
// 输入命令
hiper% revision
// 输出结果
loadname iv3300NBv486.bin 10:58:38AM-041228 user1@linux-ast.
MBID: 4420041
Feature enabled: RTC    PPPOE    VPN    IPSSG    DMZ    CBQ
Product ID: 3300VF
```

表示该产品支持 IPSSG 功能

1.2 Filter 动作

Filter 的动作包括转发和丢弃，在 HiPER 中分别用" forward=Yes "和" forward=No "来表示。当需要处理的数据包与已定义的某条 Filter 策略相匹配时，如果该策略所定义的动作是转发，那么 HiPER 将转发该数据包；如果该策略所定义的动作是丢弃，那么 HiPER 将丢弃该数据包。

未来会扩展到 proxy、log、syslog、aaa、tape 等功能。

1.3 Filter 方向

Filter 的方向包括进入和外出，在 HiPER 中分别用 " In " 和 " Out " 来表示，Filter 方向用来指出是在数据包进入或离开 HiPER 接口时对其进行过滤。Filter 的方向与数据流方向、及其应用接口密切相关，它们的涵义如下：

进入（In）— 数据包将从指定接口进入 HiPER。数据包来自与指定接口相连的网络，希望通过 HiPER 到达另一接口并从该接口转发。当指定接口接收到数据包之后，将首先进行 Filter 策略的匹配检查，如果有匹配策略，且该策略定义的动作是转发，那么将对该数据包进行路由处理；否则将直接丢弃该数据包。

外出（Out）— 数据包将从指定接口离开 HiPER。数据包来自与另一接口相连的网络，已经通过 HiPER 到达指定接口，并希望从该接口转发。当指定接口接收到数据包之后，将进行 Filter 策略的匹配检查，并根据匹配策略定义的动作处理该数据包：转发或丢弃。

从以上的介绍可以看出，Filter 方向为 In 或 Out，将导致在 HiPER 内部是先进行路由处理还是先进行 Filter 匹配检查。Filter 方向为 In 时，HiPER 将首先进行 Filter 策略的匹配检查，再进行路由处理。Filter 方向为 Out 时，HiPER 是先进行路由处理选择外出接口，再在该接口进行 Filter 策略的匹配检查。

因此，一般情况下，为了提高 HiPER 的效率，避免对将被丢弃的数据包进行路由处理，建议将 Filter 应用于与数据包源端所在网络相连（靠近）的接口，此时 Filter 方向为 In。

例如，如图 1 所示，某公司使用 HiPER 的 LAN 口连接其内部局域网，通过 WAN 口连接到公网，现要求过滤从企业内部局域网到 Internet 的流量，如果 Filter 应用于 LAN 口，其方向需定义为 In；如果 Filter 应用于 WAN 口，其方向需定义为 Out。

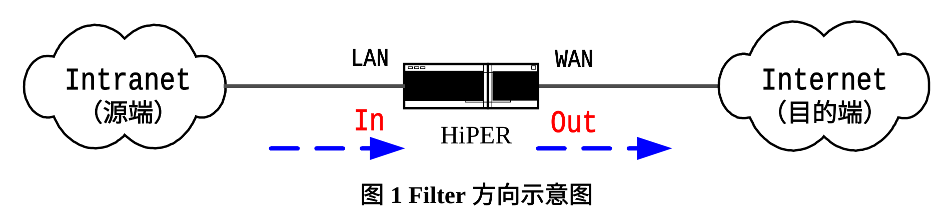


图 1 Filter 方向示意图

一般情况下，由于 HiPER 会启用 NAT 功能，所有的局域网计算机将仅使用一个或几个公网地址连接到 Internet，因此，通常都是过滤从企业内部局域网到 Internet 的流量。同时，由于一般都是 LAN 口接局域网，因此通常都是在 LAN 口启用 Filter，其方向为 In。

1.4 Filter 工作原理

当 HiPER 上没有启用 Filter 功能时，HiPER 收到没有错误的可路由的数据包，会直接根据路由表转发到相应的接口，并发送到下一跳。当定义了 Filter 策略并在某个接口启用 Filter 功能，HiPER 将会检查该接口收到或发出的每一个数据包，判断是否有符合的 Filter 策略。

所有的 Filter 策略也将按照配置的顺序依次存放在策略表中，任何后续的增加部分都放入策略表的底部。当数据包到达 HiPER 的指定接口后，HiPER 将从策略表的顶端从上至下搜索策略列表，查找是否有匹配策略，并执行匹配的第一个策略。具体地说，当配置了多个 Filter 策略时，HiPER 在指定的接口收到或者发出一个数据包时，将首先去同 Filter 策略表中的第一个策略比较，如果不匹配，那么将去同第二个策略比较，……，依此类推，一直到

匹配成功为止。如果其中的一个匹配成功，那么就执行该策略定义的动作，转发或丢弃，其余的策略就不再继续比较下去。如果与所有的 Filter 策略都不能匹配，处于安全的考虑，HiPER 将丢弃这个数据包。

Filter 策略定义前后之间是无关的，如果第一个定义的动作是转发，第二个可以是丢弃，第三个可以是转发，等等。但是由于 HiPER 将会对数据包执行第一个匹配的策略所定义的动作，因此，必须按照从特殊到一般的顺序安排、配置策略。特殊策略不排除位于列表下部的更一般性策略的应用，但位于特殊策略前的一般性策略会产生此排除效应。举个例子来说，要求禁止局域网用户使用 MSN 业务，允许其他所有业务。那么就需要先配置禁止 MSN 业务的策略，再配置允许所有业务的策略。

2　Filter 配置命令详解

2.1　增加/删除/显示 Filter 策略

【命令】

new filter {**in** | **out**}/*filter_name*
delete filter {**in** | **out**}/ *filter_name*
show filter {**in** | **out**}/ *filter_name*
show filter status {**eth1** | **eth2** | **eth3**}

【描述】

命令 **new filter** 用于新建一个 Filter 策略；
命令 **delete filter** 用于删除一个指定 Filter 策略；
命令 **show filter** 用于显示一个指定 Filter 策略的配置信息；
命令 **show filter status** {**eth1** | **eth2** | **eth3**}用于显示指定接口当前 Filter 策略的工作状态。注意：REL480 以后（包括 480）版本才支持这条命令。
如果需要查看所有已配置的 Filter 策略的相关信息，则需要使用命令 **show running** 来查看。

【参数】

in：表示过滤方向为进入，即对从指定接口进入 HiPER 的数据包进行过滤；
out：表示过滤方向为外出，即对从指定接口离开 HiPER 的数据包进行过滤；
filter_name：预定义的策略的名称，用户自定义；
eth1：表示 LAN 口；
eth2：表示 WAN 口；
eth3：表示 WAN2/DMZ 口，仅双 WAN 口产品支持。

【实例】

//创建一个新 Filter 策略，该策略的名称为 test，方向为进入。
new filter in/test
//删除一个名称为 test 的 Filter 策略，该策略方向为进入。
delete filter in/test
//显示一个名称为 test 的 Filter 策略，该策略方向为进入。
show filter in/test
//显示 LAN 口当前 Filter 策略的工作状态。

show filter stauts eth1

2.2 配置 Filter

2.2.1 定义 Filter 类型

【命令】

set filter {**in** | **out**}/ *filter_name* **type** {**ip** | **ipssg** | **generic**}

【描述】

命令 **set filter** {**in** | **out**}/ *filter_name* **type** 用于定义预配置的 filter 策略的类型。

【参数】

ip：预配置的 Filter 策略的类型为 IP Filter；
ipssg：预配置的 Filter 策略的类型为 IPSSG Filter；
generic：预配置的 Filter 策略的类型为 IPSSG Filter。

【实例】

// 预配置策略的类型为 IPSSG Filter，该策略的名称为 test，方向为进入。
set filter in/test type ipssg

2.2.2 定义 Filter 动作

【命令】

set filter {**in** | **out**}/ *filter_name* **forward** {**yes** | **no**}

【描述】

命令 **set filter** {**in** | **out**}/ *filter_name* **forward** 用于定义预配置的 Filter 策略的动作。

【参数】

Yes：表示允许，与此策略匹配的数据包将被转发；
No：表示禁止，与此策略匹配的数据包将被丢弃。

【实例】

// 预配置策略的动作为允许，该策略的名称为 test，方向为进入。
set filter in/test forward yes

2.2.3 配置 IP Filter

【命令】

set filter {**in** | **out**}/ *filter_name* **IP** {**SrcMask** *SrcMask* | **ScrAddr** *ScrAddr* | **DestMask** *DestMask* | **DestAddr** *DestAddr* | **Protocol** *Protocol* | **ScrPortCmp** {**None** | **Less** | **Eql** | **Gtr** | **Neq** } | **SrcPort** *SrcPort* | **DestPortCmp** {**None** | **Less** | **Eql** | **Gtr** | **Neq** } | **DestPort** *DestPort* | **TcpEstab** {**Yes** | **No**}}

【描述】

命令 **set filter** {**in** | **out**}/ *filter_name* **IP** 用于配置类型为 IP Filter 的策略。

【参数】

SrcMask：指定源 IP 掩码；
SrcMask：数据包的源 IP 地址掩码，点分十进制表示。

ScrAddr：指定源 IP 地址（主机地址或网络号）；
ScrAddr：数据包的源 IP 地址，点分十进制表示。

DestMask：指定目的 IP 掩码；
DestMask：数据包的目的 IP 地址掩码，点分十进制表示。

DestAddr：指定目的 IP 地址（主机地址或网络号）；
DestAddr：数据包的目的 IP 地址，点分十进制表示。

Protocol：指定协议类型；
Protocol：数据包的协议类型，用数字表示。如：UDP 为 17，TCP 为 6。缺省值为 0，表示任意协议。

ScrPortCmp：指定 UDP 或 TCP 报文的源端口匹配动作，仅在规则指定的协议类型是 TCP 或 UDP 时有效。**None—**无动作，**Less—**小于，**Eql—**等于，**Gtr—**大于，**Neq—**不等于。

SrcPort：指定 UDP 或者 TCP 报文的源端口号，仅在规则指定的协议类型是 TCP 或 UDP 时有效；如果不指定，表示 TCP/UDP 报文的任何源端口信息都匹配；
Srcport：TCP 或 UDP 报文的源端口号，用数字表示，取值范围为 1~65535。

DestPortCmp：指定 UDP 或 TCP 报文的目的端口匹配动作，仅在规则指定的协议类型是 TCP 或 UDP 时有效。**None—**无动作，**Less—**小于，**Eql—**等于，**Gtr—**大于，**Neq—**不等于。

DestPort 指定 UDP 或者 TCP 报文的目的端口号,仅在规则指定的协议类型是 TCP 或 UDP 时有效；如果不指定，表示 TCP/UDP 报文的任何目的端口信息都匹配；
DestPort：TCP 或 UDP 报文的目的端口号，用数字表示，取值范围为 1~65535。

TcpEstab：指定 TCP 连接发起方向，仅适用于 TCP 协议。**Yes—**连接必须为出连接；**No—**不限制连接方向，连接可以是远端发起，缺省值为 **No**。

【使用指南】

1. 过滤源 IP 地址和目的 IP 地址的方法

可通过配置参数 **SrcMask**、**ScrAddr** 来过滤源 IP 地址，通过配置参数 **DestMask**、**DestAddr** 来过滤目的地址。二者的配置方法完全相同，这里以如何过滤源 IP 地址为例进行说明。
注意：此处的地址掩码采用相同于 TCP/IP 的子网掩码相同的规则，具体来说就是掩码为 1 的位要严格匹配，掩码为 0 的为不需匹配。

1) 如果要配置单机用户，则需将 **SrcMask** 设为 255.255.255.255，**ScrAddr** 为该主机的 IP 地址；
2) 如果要配置一段范围的 IP 地址，则需将 **SrcMask** 设为这段地址的子网掩码，**ScrAddr** 为该范围内任意一个 IP 地址。例如如果某策略的源 IP 地址范围为 192.168.1.1～192.168.1.31，则需将 **SrcMask** 设为 255.255.255.224。
3) **SrcMask** 设为 0.0.0.0，且 **ScrAddr** 设为 0.0.0.0 时，代表所有的 IP 地址。

2. 过滤源端口和目的端口的方法

只有在指定的协议类型是“TCP”或“UDP”之后，即将 **Protocol** 设为 6 或 17 之后，端口配置才有效。如果协议类型设置为“0”(表示任意协议)，那么将无法取

到包的端口信息，从而所有端口设置将被忽略。

可通过参数 **SrcPort** 和 **SrcPortCmp** 配置源端口，通过参数 **DestPort** 和 **DestPortCmp** 配置目的端口。二者的配置方法完全相同，这里以如何过滤源端口为例进入说明。

1) 如果要配置单个端口，只需将 **SrcPort** 设置为指定端口号，将 **SrcPortCmp** 设为 **Eql**（即等于）即可。
2) 配置一段范围的端口，有以下三种情况：
    a) 如果要配置的端口范围为大于某个端口号的所有端口，只需将 **srcPort** 设置为指定端口号，并将 **SrcPortCmpp** 设为 **Gtr**（即大于）即可。
    b) 如果要配置的端口范围为小于某个端口的所有端口，只需将 **srcPort** 设置为指定端口号，并将 **SrcPortCmp** 设为 **Less**（即小于）即可。
    c) 如果要配置某段范围内的端口，则需要通过配置两个策略实现，即将上述 b、c 所述结合起来使用。

3. 常用服务及对应端口号

FTP（Port:21）、TELNET（Port:23）、SMTP（Port:25）；
DNS（Port:53）、FINGER（Port:79）、HTTP（Port:80）；
POP3（Port:110）、NNTP（Port:119）、SNMP（Port:161）。

4. TCP 连接方向的控制

一般情况下，无需控制 TCP 连接方向。如果希望 TCP 连接只能由内网主机建立连接，以保证内网主机不提供网络服务，就需要限制 TCP 连接方向，以实现单向访问连接。参数 **TcpEstab** 的缺省值为 **No**，表示不限制连接方向；只需将 **TcpEstab** 设置为 **Yes**，即可指定连接方向，表示 TCP 连接为出连接时，才匹配该策略。

比如希望禁止来自 Internet 的 telnet 访问，但是允许内部主机 telnet 访问 Internet 中的主机，这时就需要限制 TCP 连接方向，将 **TcpEstab** 设置为 **Yes**。

【实例】

实例 1

// 增加一个 Filter 策略，要求允许 IP 地址在 192.168.1.1～192.168.1.31 范围之内的主机上网。

```
new filter in/1
set filter in/1 type ip
set filter in/1 forward yes
set filter in/1 ip srcmask 255.255.255.224
set filter in/1 ip srcaddr 192.168.16.1
```

实例 2

// 增加一个 Filter 策略，要求禁止内网主机访问网站 209.247.228.201。

```
new filter in/a
set filter in/a type ip
set filter in/a forward no
set filter in/a ip destmask 255.255.255.255（单个地址掩码为 255.255.255.255）
set filter in/a ip destaddr 209.247.228.201
```

实例 3

// 增加一个 Filter 策略，要求禁止内网用户使用端口 1863。

```
new filter in/2
set filter in/2 type ip
set filter in/2 forward no
set filter in/2 ip protocol 6
set filter in/2 ip destportcmp eql
set filter in/2 ip destport 1863
```

实例 4

// 增加一个 Filter 策略，禁止内网用户使用端口 4600～4800。

首先允许使用端口号小于 4600 的所有端口,然后禁止使用端口号小于 4800 的所有端口，这样端口号位于 4600～4800 之间的所有端口将被禁止，而端口号大于 4800 的所有端口将被允许。

```
// 允许小于 4600
new filter in/3
set filter in/3 type IP
set filter in/3 forward yes
set filter in/3 ip protocol 6
set filter in/3 ip destportcmp less
set filter in/3 ip destport 4600
```

```
// 禁止小于 4800
new filter in/4
set filter in/4 type IP
set filter in/4 forward no
set filter in/4 ip protocol 6
set filter in/4 ip destportcmp less
set filter in/4 ip destport 4800
```

2.2.4 配置 GENERIC Filter

【命令】

set filter {**in** | **out**}**/** *filter_name* **Generic**{**Offset** *Offset* | **Length** *Length* | **Mask** *Mask* | **Value** *Value* | **Compare** {**Equals** | **NotEquals** } | **More** {**Yes** | **No** }}

【描述】

命令 **set filter** {**in** | **out**}**/** *filter_name* **Generic** 用于配置 GENERIC Filter 类型的策略。

【参数】

Offset：指定偏移量，即数据包需要比较的内容的起始位置距离包头（包括以太网包头）的字节数；
Offset：偏移量，单位为字节数，取值范围：0-1500。

Length：指定数据包需要比较的长度；
Length：数据包比较的长度，单位为字节数，取值范围：0-8。

Mask：指定匹配掩码；
Mask：数据包需要比较的内容的掩码，16 进制格式输入，与 **value** 位数相同。

Value：指定匹配值，即数据包中需要比较的内容；对于 **Value** 来说，**Mask** 为“ 1 ”（2 进制）的地址位需严格匹配，为“ 0 ”（2 进制）的地址位无需匹配；

Value：数据包需要比较的内容，16 进制格式输入。

Compare：指定数据包匹配动作。**Equals—**表示指定比较内容相同时匹配，**NotEquals—**表示指定比较内容不同时匹配，缺省值为 **Equals。**

More：指定是否需要检查后续策略。**Yes—**表示还需要检查后续策略，**No—**表示无需检查后续策略，缺省值为 **Yes**。

【使用指南】

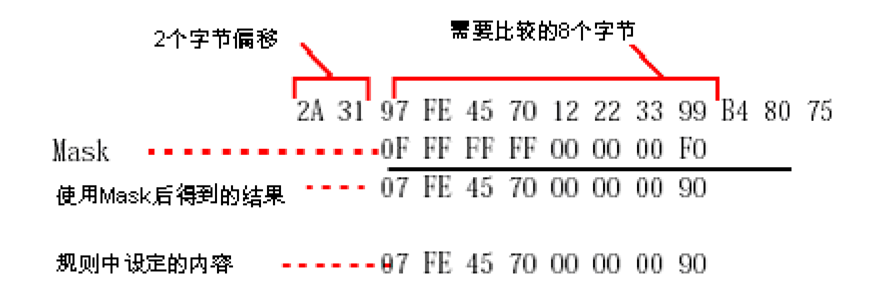
Generic Filter 是依据数据包的内容来配置 Filter 策略的。具体地讲，首先通过指定偏移量（Offset）来确定从数据包的哪一位开始比较；然后指定要比较内容的长度（Length）；再通过设置数据包的匹配值（Value）和掩码（Mask）来指定需要检查的比特位，要比较的内容中，掩码为“ 1 ”（2 进制）的地址位需严格匹配，掩码为“ 0 ”（2 进制）的地址位将被忽略。

【实例】

```
//  过滤参数如下所述：
    offset = 2
    length = 8
    more = no
    compare= equals
    mask = 0f:ff:ff:ff:00:00:00:f0
    value = 07:fe:45:70:00:00:00:90
// 新建一个 Genric 策略，禁止符合上述过滤参数的数据包通过；
   new filter in/test
   set filter in/test type generic
   set filter in/test forward no
   set filter in/test generic offset 2
   set filter in/test generic lenth 8
   set filter in/test generic more no
   set filter in/test generic compare equals
   set filter in/test generic mask 0fffffff000000f0
   set filter in/test generic value 07fe457000000090
```

// 假设有个包开始的内容如下：2A 31 97 FE 45 70 12 22 33 99 B4 80 75

当该数据包和上述 Generic Filter 策略相比较时，因为 offset 是 2，长度 length 为 8，所以需要比较从第三个字节 97 开始的 8 个字节中的内容，直到第 10 个字节结束。这 8 个字节中，只检查与 Mask 为“ 1 ”对应的地址位，忽略与“ 0 ”对应的地址位，计算方式如下：



2.2.5 配置 IPSSG Filter

【命令】

set filter {**in** | **out**}/ *filter_name* **IPSSG** {**TimeRange** *Time_Name* | **EType** *EType* | **ENeq** {**Equals** | **NotEquals**} | **SMac** *SMac* | **SNeq** {**Equals** | **NotEquals**} | **DMac** *DMac*| **DNeq** {**Equals** | **NotEquals**} | **SrcMask** *SrcMask* | **SrcAddr** *SrcAddr* | **SrcFrom** *SrcFrom* | **SrcEnd** *SrcEnd* | **DestMask** *DestMask* | **DestAddr** *DestAddr* | **DestFrom** *DestFrom* | **DestEnd** *DestEnd* | **Protocol** *Protocol* | **SrcPortCmp** {**None** | **Less** | **Eql** | **Gtr** | **Neq** } | **SrcPort** *SrcPort* | **SportFrom** *SportFrom* | **SportEnd** *SPortEnd* | **DestPortCmp** {**None** | **Less** | **Eql** | **Gtr** | **Neq** } | **DestPort** *DestPort* | **DportFrom** *DportFrom* | **DportEnd** *DportEnd* | **TcpEstab** {**Yes** | **No**}}

【描述】

命令 **set filter** {**in** | **out**}/ *filter_name* **IPSSG** 用于配置类型为 IPSSG Filter 的策略。

【参数】

TimeRange：指定策略的生效时间。如果没有指定，表示该策略不受时间限制，一直有效；如果指定了，则表示该策略仅仅在指定的时间段范围内有效；
Time_Name：策略生效的时间段实例名，时间段的配置参考本章 2.2.6 节。

EType：指定以太网数据帧的类型；
EType：以太网数据帧的类型，一个 16 比特的十六进制数。缺省值为 0 ，代表不检查以太网类型。

ENeq：以太网数据帧的类型的比较符，**Equals**——等于，表示类型相同时匹配；**NotEquals**——不等于，表示类型不同时匹配。

SMac：指定源 MAC 地址；
SMac：数据包的源 MAC 地址，MAC 地址由 48 位 2 进制数组成。采用 16 进制格式输入，共 12 个字符。

SNeq：源 MAC 地址比较符，**Equals** 表示等于，也就是数据包的源 MAC 地址与指定值相等时匹配；**NotEquals** 表示不等于，也就是数据包的源 MAC 地址与指定值不相等时匹配。

DMac：指定目的 MAC 地址；
DMac：数据包的源 MAC 地址，输入格式同 DMac。

DNeq：目的 MAC 地址比较符，**Equals** 表示等于，也就是数据包的目的 MAC 地址与指定值相等时匹配；**NotEquals** 表示不等于，也就是数据包的目的 MAC 地址与指定值不相等时匹配。

SrcMask：指定源 IP 掩码；
SrcMask：数据包的源 IP 地址掩码，点分十进制表示。

SrcAddr：指定源 IP 地址（主机地址或网络号）；
SrcAddr：数据包的源 IP 地址，点分十进制表示。

SrcFrom：指定起始源 IP 地址（主机地址）；
SrcFrom：数据包的起始源 IP 地址，点分十进制表示。

SrcEnd：指定结束源 IP 地址（主机地址）；
SrcEnd：数据包的结束源 IP 地址，点分十进制表示。

DestMask：指定目的 IP 掩码；
DestMask：数据包的目的 IP 地址掩码，点分十进制表示。

DestAddr：指定目的 IP 地址（主机地址或网络号）；
DestAddr：数据包的目的 IP 地址，点分十进制表示。

DestFrom：指定起始目的 IP 地址（主机地址）；
DestFrom：数据包的起始目的 IP 地址，点分十进制表示。

DestEnd：指定结束目的 IP 地址（主机地址）；
DestEnd：数据包的结束目的 IP 地址，点分十进制表示。

Protocol：指定协议类型；
Protocol： 数据包的协议类型，用数字表示，如：UDP 为 17，TCP 为 6。缺省值为 0，表示任意协议。

SrcPortCmp：指定 UDP 或 TCP 报文的源端口匹配动作，仅在规则指定的协议类型是 TCP 或 UDP 时有效。**None**—无动作，**Less**—小于，**Eql**—等于，**Gtr**—大于，**Neq**—不等于。

SrcPort：指定 UDP 或者 TCP 报文的源端口号，仅在规则指定的协议类型是 TCP 或 UDP 时有效；
SrcPort：TCP 或 UDP 报文的源端口号，用数字表示，取值范围为 1~65535。

SportFrom：指定 TCP 或者 UDP 报文的起始源端口号，仅在规则指定的协议类型是 TCP 或 UDP 时有效；
SportFrom：TCP 或 UDP 报文的起始源端口号，用数字表示，取值范围为 1~65535。

SportEnd：指定 TCP 或者 UDP 的结束源端口号，仅在规则指定的协议类型是 TCP 或 UDP 时有效；
SportEnd：TCP 或 UDP 报文的结束源端口号，用数字表示，取值范围为 1~65535。

DestPortCmp：指定 UDP 或 TCP 报文的目的端口匹配动作，仅在规则指定的协议类型是 TCP 或 UDP 时有效。**None**—无动作，**Less**—小于，**Eql**—等于，**Gtr**—大于，**Neq**—不等于。

DestPort：指定 UDP 或者 TCP 报文的目的端口号，仅在规则指定的协议类型是 TCP 或 UDP 时有效；
DestPort：TCP 或 UDP 报文的目的端口号，用数字表示，取值范围为 1~65535。

DportFrom：指定 UDP 或者 TCP 报文的起始目的端口号，仅在规则指定的协议类型是 TCP 或 UDP 时有效；
DportFrom：TCP 或 UDP 报文的起始目的端口号，用数字表示，取值范围为 1~65535。

DportEnd：指定 UDP 或者 TCP 报文的结束目的端口号，仅在规则指定的协议类型是 TCP 或 UDP 时有效；

DportEnd：TCP 或 UDP 报文的结束目的端口号，用数字表示，取值范围为 1~65535。

TcpEstab：指定 TCP 连接发起方向，仅适用于 TCP 协议。**Yes**—连接必须为出连接；**No**—不限制连接方向，连接可以是远端发起。

【使用指南】

1. 过滤源 IP 地址和目的 IP 地址的方法

方法一：

通过配置参数 **SrcMask**、**SrcAddr** 来过滤源 IP 地址，通过配置参数 **DestMask**、**DestAddr** 来过滤目的地址。具体方法同 IP Filter，请参考章节 2.2.3 中 IP Filter 的使用指南。

方法二：

通过配置参数 **SrcFrom** 和 **SrcEnd** 来过滤源 IP 地址，通过配置参数 **DestFrom** 和 **DestEnd** 来过滤目的 IP 地址。二者的配置方法完全相同，这里以过滤目的 IP 地址为例进行说明。

1) 如果要过滤单个地址，则需将 **DestFrom** 和 **DestEnd** 均设为预指定的 IP 地址；
2) 如果要过滤一段范围的 IP 地址，则需将 **DestFrom** 设为这段地址的起始地址，将 **DestEnd** 设为这段地址的结束地址。例如如果某策略需要过滤的源 IP 地址范围为 218.1.1.2～218.1.1.5，则需将 **DestFrom** 和 **DestEnd** 分别设为 218.1.1.2、218.1.1.5。

2. 过滤源端口和目的端口的方法

只有在指定的协议类型是“ TCP ”或“ UDP ”之后，即将 **Protocol** 设为 6 或 17 之后，端口配置才有效。如果协议类型设置为“ 0 ”（表示任意协议），那么将无法取到包的端口信息，从而所有端口设置将被忽略。

方法一：

可通过配置参数 **SrcPort** 和 **SrcPortCmp** 来过滤源端口，通过配置参数 **DestPort** 和 **DestPortCmp** 来过滤目的端口。具体方法同 IP Filter，请参考章节 2.2.3 中 IP Filter 的使用指南。

方法二：

可通过配置参数 **SportFrom** 和 **SportEnd** 来过滤源端口，通过配置参数 **DportFrom** 和 **DportEnd** 配置目的端口。二者方法完全相同，这里以指定目的端口为例进行说明。

1) 如果要过滤单个端口，则需将 **DportFrom** 和 **DportEnd** 均设为预指定的端口；
2) 过滤一段范围的端口，有以下三种情况：
   a) 如果要过滤某段范围内的端口（包括起始端口和结束端口），则需将 **DportFrom** 设为起始端口，将 **DportEnd** 设为结束端口。
   b) 如果要过滤的端口范围为大于某个指定端口号的所有端口（包括该指定端口），则需将 **DportFrom** 设为指定端口，并将 **DportEnd** 设为 **65535**。
   c) 如果要过滤的端口范围为小于某个指定端口的所有端口（包括该指定端口），则需将 **DportFrom** 设为 0，并将 **DportEnd** 设为指定端口。

3. TCP 连接方向的控制

TCP 连接方向的用法同 IP Filter，请参考章节 2.2.3 中 IP Filter 的使用指南。

4. 过滤源 MAC 地址和目的 MAC 地址的方法

可通过配置参数 **SMac** 和 **SNeq 来**过滤源 MAC 地址,通过配置参数 **DMac** 和 **Dneq 来**过滤目的 MAC 地址。二者的配置方法相同，这里以过滤源 MAC 地址为例进行说明。

当 **SNeq** 为 **Equals** 时，表示数据包的源 MAC 地址与指定 MAC 地址相等时匹配；当 **SNeq** 为 **NotEquals** 时，表示数据包的源 MAC 地址与指定 MAC 地址不相等时匹配。

【注意事项】

以下几个参数，REL460 以后（包括 460）的版本开始支持。

SrcFrom [源起始 IP]、**SrcEnd** [源结束 IP]、**DestFrom** [目的起始 IP]、**DestEnd** [目的结束 IP]、**SportFrom** [源起始端口]、**SportEnd** [源结束端口]、**DportFrom** [目的起始端口]、**DportEnd** [目的结束端口]

【实例】

实例 1

// 增加一个 Filter 策略，要求允许 IP 地址在 192.168.1.1～192.168.1.31 范围之内的主机上网。

```
new filter in/permit1
set filter in/permit1 type ipssg
set filter in/permit1 forward yes
set filter in/permit1 ipssg srcfrom 192.168.1.1
set filter in/permit1 ipssg srcend 192.168.1.31
```

实例 2

// 增加一个 Filter 策略，禁止内网用户使用端口 4600～4800。

```
new filter in/denyport1
set filter in/denyport1 type ipssg
set filter in/denyport1 forward no
set filter in/denyport1 ipssg protocol 6
set filter in/denyport1 ipssg destFrom 4600
set filter in/denyport1 ipssg destEnd 4800
```

实例 3

// 增加一个 Filter 策略，禁止内网中 MAC 地址为 00:07:95:a8:1c:3d 的主机上网。

```
new filter in/denymac1
set filterin/denymac1 type ipssg
set filter in/denymac1 forward no
set filter in/denymac1 ipssg smac 000795a81c3d
set filter in/denymac1 ipssg sneq equals
```

实例 4

// 增加一个 Filter 策略，实现 IP/MAC 绑定，例如：禁止 IP 地址为 192.168.1.150，MAC 地址不为 004c5aeefcff 的主机上网。

```
new filter in/binding1
```

set filter in/binding1 type ipssg

set filter in/binding1 forward no

set filter in/binding1 ipssg srcmask 255.255.255.255

set filter in/binding1 ipssg srcaddr 192.168.1.150

set filter in/binding1 ipssg smac 004c5aeefcff

set filter in/binding1 ipssg sneq notequlas

注意：在 440 版本以后，可以通过 IP/MAC 绑定实现与实例 4 同样的功能，而且效率更高。

2.2.6 配置时间段

【命令】

new TimeRange/*Time_Name*

set TimeRange/*Time_Name* { **Enabled | Disabled** }

set TimeRange/*Time_Name* {**TmStart** *date1 time1*| **TmStop** *date2 time2*}

set TimeRange/*Time_Name* {**1stperiod | 2ndperiod | 3rdperiod | 4thperiod | 5thperiod | 6thperiod | 7thperiod | 8thperiod** } {**Type** *days_of_week* | **Begin** *begin_time*| **End** *end_time*}

delete TimeRange/*Time_Name*

【描述】

命令 **new TimeRange** 用于新建一个时间段；

命令 **set TimeRange** 用于配置一个指定时间段；

命令 **delete TimeRange** 用于删除一个指定时间段。

【参数】

Time_Name：时间段名称，用户自定义。

TmStart：指定时间段生效的起始时刻（日期和时间）；如果不设置起始时间，表示不关心起始时间，只关心结束时间，即时间立即生效；

date1：时间段生效的起始日期，输入格式为年-月-日，缺省值为 1990-1-1；

time1：时间段生效的起始时间，输入格式为小时:分钟:秒，采用 24 小时时钟来表示，缺省值为 0:00:00。

TmStop：指定时间段生效的结束时刻（日期和时间）。其中 *date2* 和 *time2* 的输入格式与起始时间相同。结束时间必须大于起始时间，如果没有设置结束时间，则结束时间为系统最大可能时间。起始日期和时间、结束日期和时间均为缺省值，即 1990-1-1 0:00:00 时，表示该时间段永远有效。

1stperiod、**2ndperiod**、**3rdperiod**、**4thperiod**、**5thperiod**、**6thperiod**、**7thperiod**、**8thperiod**：指定时间段的时间单元，一个时间段最多可配 8 个时间单元。

Type：指定预配置的时间单元在一周的哪一（几）天有效；

days_of_week：时间单元在每星期的有效日，可以输入以下参数：**None**、**Everyday**、**Monday**、**Tuesday**、**Wednesday**、**Thursday**、**Friday**、**Saturday**、**Sunday**、**Weekday**、**Weekend**，其中 **Monday**、**Tuesday**、**Wednesday**、**Thursday**、**Friday**、**Saturday**、**Sunday** 分别表示星期一、星期二、星期三、星期四、星期五、星期六、星期天；**Everyday** 表示每一天，包括一周七天；**Weekday** 表示工作日，包括从星期一到星

期五共五天；**Weekend** 表示周末，包括星期六、星期天两天；缺省值为 **None**，表示未定义。

Begin：指定预配置时间单元生效的起始时刻；
begin_time：时间单元生效的起始时刻，输入格式为小时**:**分钟**:**秒，采用 24 小时时钟来表示。

End：指定预配置时间单元生效的结束时刻；
end_time：时间单元生效的结束时刻，输入格式同 *begin_time*。

【使用指南】

1. 对于每个时间段来说，可以配置 8 个时间单元。配置时间段信息时，首先通过 **TmStart** 和 **TmStop** 来指定该时间段的有效时间范围。然后针对每个时间段，分别配置其时间单元，每个时间单元通过 **Begin** 和 **End** 参数来指定以一周为间隔的周期性时间，同时结合 **Type** 参数指明在每周的星期几生效。
2. 为保证时间工作正常，在使用时间段相关功能之前，首先必须校正系统时钟。在 HiPER 中，既可以通过手动设置时间；也可以通过 sntp 协议，自动询问标准的 sntp 服务器取得当前时间，并通过设置时区 **time-zone** 来设置当前的时区，来获得准确的全球时间。
   1) 手动方式
      设置系统日期时间
      set system datatime *yyyy-mm-dd hh:mm:ss*
   2) 自动方式
      a) 设置时区
         set system timezone *timezone*
      b) 启用 sntp 服务器
         set ip sntp enabled {**Yes** | **No**}
         Yes 表示启用，**No** 表示禁用，缺省值为 **No**。
         注意：在使用手动方式时，此处需设置为 **No**。
      c) 设置 sntp 服务器的 IP 地址，最多可以设置 3 个 sntp 服务器
         set ip sntp {**1stsntpserver** | **2ndsntpserver** | **3rdsntpserver** } *sntpserver_IP*

【实例】

// 手动校正系统时间实例
// 当前时间为 2004 年 12 月 27 日，12 点 30 分 15 秒。
set system datatime 2004-12-27 12:30:15

// 自动校正系统时间实例
// HiPER 使用地点为中国北京，可使用两个 sntperver，IP 地址分别为：137.107.1.10 和 128.250.36.2。
set system time zone UTC+0800
set ip sntp enabled Yes
set ip sntp 1stsntpserver 192.43.244.18
set ip sntp 2ndsntpserver 129.6.15.28

// 配置时间段实例

// 该时间段名称定义为 work，在 2004 年度有效。
new timerange/work
set timerange/work Tmstart 2004-1-1 0:00:00
set timerange/work Tmstop 2004-12-31 23:59:59
// 该时间段由 2 个时间单元组成：星期一至星期五，09:00:00～11:59:59；星期六～星期天 13:00:00～17:59:59。
set timerange/work 1stperiod type weekday
set timerange/work 1stperiod begin 09:00:00
set timerange/work 1stperiod end 11:59:59
set timerange/work 2ndperiod type weekday
set timerange/work 2ndperiod begin 13:00:00
set timerange/work 2ndperiod end 17:59:59

// 删除时间段实例
// 删除一个名称为 free 的时间段
delete timerange/free

2.3 启用/禁用 Filter

【命令】

set interface ethernet/{**1** | **2** | **3** } **IP Filter** {**Enabled** | **Disabled** }

【描述】

该命令用于在路由器指定接口启用或禁用 Filter 策略。

【参数】

1：指定 Filter 策略作用于路由器 LAN 口；
2：指定 Filter 策略作用于路由器 WAN 口；
3：指定 Filter 策略作用于路由器 WAN2/DMZ 口（仅双 WAN 口产品支持）；
Enabled：在指定接口启用 Filter 策略；
Disabled：在指定接口禁用 Filter 策略，为缺省值。

【使用指南】

在定义了 Filter 策略后，必须在需要 Filter 功能的接口，启用 Filter，否则所定义的 Filter 策略根本不会执行。

【实例】

// 在 LAN 口启用 Filter 策略
set interface ethernet/1 IP Filter Enabled

3 Filter 策略配置步骤

3.1 配置步骤

1. 配置各局部策略；

1） 新建一条策略，确定 Filter 方向，自定义策略名；
2） 定义 Filter 类型；
3） 定义 Filter 动作；
4） 配置其余 Filter 参数。

2. 配置全局策略；

处于安全考虑，HiPER 的策略体系中默认全局策略的动作是禁止，即与所有 Filter 策略均不匹配的数据包将被丢弃。因此，一般情况下，在配置完所有的局部策略后，需要在策略表的最后配置一条全局策略，用来允许其余所有无匹配策略的数据包通过，以保证局域网用户正常上网。

全局策略配置方法如下所述：

// 配置全局策略，允许所有没有匹配策略的数据包通过，假设该策略名为 other，方向为进入。

```
new filter in/other
set filter in/other type GENERIC
set filter in/other forward yes
```

3. 在指定接口启用 Filter 策略。

在配置完所有的 Filter 策略后，还需为 Filter 策略指定其作用接口，才能启用 Filter，否则 Filter 策略将不起任何作用。

// 在 LAN 口启用 Filter

```
set interface ethernet/1 IP Filter Enabled
```

4. 保存配置

所有的配置完成之后，还需输入命令：**Write**，用以保存配置。只有执行 **Write** 命令之后，配置才会生效。

3.2 增加一条 Filter 策略

如章节 1.4 所述，所有的 Filter 策略是按照配置的先后顺序存放在策略表中的，而 HiPER 在启用 Filter 之后，当指定接口有数据包通过时，将按照策略表的顺序依次检查 Filter 策略，看是否由匹配策略。

如果已经配置了多条策略，现需要在其中某条策略的前面增加一条策略，则需要按以下步骤进行：

1. 在指定接口关闭 Filter；
2. 删除全局策略；
3. 删除从新增策略插入位置开始的那一条至最后一条之间对应的所有局部策略；
4. 增加新策略；
5. 按照原先的配置顺序依次增加那几条被删除的局部策略；
6. 增加被删除的全局策略；
7. 在指定接口启用 Filter；
8. 保存上述配置。

实例，假设某用户已经按顺序配置了四条局部策略（策略名为 1、2、3、4）以及全局策略（策略名为 Generic）。如下所示，具体配置略。

new filter in/1
……
new filter in/2
……
new filter in/3
……
new filter in/4
……
new filter in/Generic
……
set interface ethernet/1 ip filter enabled

现在希望在第 3 条策略前加入一条策略（策略名为 5），步骤如下：

1. 在指定接口关闭 filter
   set interface ethernet/1 ip filter disabled
2. 删除全局策略 Generic
   deleteete filter in/Generic
3. 删除局部策略 4 和 3
   deleteete filter in/4
   deleteete filter in/3
4. 增加局部策略 5
   new filter in/5
   ……
5. 增加被删除的局部策略 4 和 3
   new filter in/3
   ……
   new filter in/4
   ……
6. 增加被删除的全局策略 Generic
   new filter in/Generic
   ……
7. 在指定接口启用 filter
   set interface ethernet/1 ip filter enabled
8. 保存上述配置
   write

3.3 删除一条 Filter 策略

如果已经配置了多条策略，现需要删除其中的某条策略，则需要按以下步骤进行：

1. 在指定接口关闭 Filter；
2. 删除全局策略；
3. 删除策略表中预被删除的策略至最后一条之间对应的所有局部策略；
4. 按照原先的配置顺序依次增加那几条删除的局部策略，当然，预被删除的策略除外；
5. 增加被删除的全局策略；

6. 在指定接口启用 Filter；
7. 保存上述配置。

实例，假设某用户已经按顺序配置了四条局部策略（策略名为 1、2、3、4）以及全局策略（策略名为 Generic）。如下所示，具体配置略。

```
new filter in/1
……
new filter in/2
……
new filter in/3
……
new filter in/4
……
new filter in/Generic
……
set interface ethernet/1 ip filter enabled
```

现在希望删除策略 2，步骤如下：

1. 在指定接口关闭 filter
   set interface ethernet/1 ip filter disabled
2. 删除全局策略 Generic
   deleteete filter in/Generic
3. 删除局部策略 4、3 和 2
   deleteete filter in/4
   deleteete filter in/3
   deleteete filter in/2
4. 增加被删除的局部策略 4 和 3
   new filter in/3
   ……
   new filter in/4
   ……
5. 增加被删除的全局策略 Generic
   new filter in/Generic
   ……
6. 在指定接口启用 filter
   set interface ethernet/1 ip filter enabled
7. 保存上述配置
   write

4 Filter 策略配置实例

4.1 对目的 IP 地址过滤

4.1.1 要求 1：禁止局域网用户访问外网某些网站，允许其他业务

实例 1：

国家有关部门可通过 IP Filter 来禁止国内用户去访问那些违反我国有关规定或者"有问题"的国外站点，例如 http://www.playboy.com、http://www.cnn.com 等等。

www.playboy.com 对应的 IP 地址为 209.247.228.201，

www.cnn.com 对应的 IP 地址为 64.236.24.12

具体配置如下：

```
// 配置禁止访问 www.playboy.com 的策略
// 新建 filter 策略 1（局部设置）
   new filter in/1
   set filter in/1 type ip
   set filter in/1 forward no
// 设置要过滤的目的 IP 地址 209.247.228.201（通过 IP 地址和子网掩码定位需要过滤的 IP
   地址段）
   set filter in/1 ip destmask 255.255.255.255（单个地址掩码为 255.255.255.255）
   set filter in/1 ip destaddr 209.247.228.201

// 配置禁止访问 www.cnn.com 的策略
// 新建 filter 策略 2（局部设置）
   new filter in/2
   set filter in/2 type ip
   set filter in/2 forward no
// 设置要过滤的目的 IP 地址 64.236.24.12
   set filter in/2 ip destmask 255.255.255.255
   set filter in/2 ip destaddr 64.236.24.12

// 设置全局策略，允许其他所有数据包（必须有，且最后设置）
   new filter in/3
   set filter in/3 type generic
   set filter in/3 forward yes

// 在 LAN 口上启用 Filter
   set interface ethernet/1 ip filter enabled

// 保存上述配置
   write
```

4.1.2 要求 2：允许局域网用户访问某些网站，禁止访问其他网站

实例 2：

只允许内网用户访问以下地址段的网站，202.0.0.0/8，218.0.0.0/8，211.0.0.0/8，其他网段不允许访问。

具体配置如下：

// 允许访问 202.0.0.0/8
// 新建 filter 策略 1（局部设置）
new filter in/1
set filter in/1 type ip
set filter in/1 forward yes
// 设置要过滤的目的网络的 IP 地址 202.0.0.0/8（通过 IP 地址和子网掩码定位需要过滤的 IP 地址段）
set filter in/1 ip destmask 255.0.0.0（该网段为 C 类子网）
set filter in/1 ip destaddr 202.0.0.0

// 允许访问 218.0.0.0/8
// 新建 filter 策略 2（局部设置）
new filter in/2
set filter in/2 type ip
set filter in/2 forward yes
// 设置要过滤的目的地址 218.0.0.0
set filter in/2 ip destmask 255.0.0.0
set filter in/2 ip destaddr 218.0.0.0

// 允许访问 211.0.0.0/8
// 新建 filter 策略 3（局部设置）
new filter in/3
set filter in/3 type ip
set filter in/3 forward yes
// 设置要过滤的目的地址 211.0.0.0
set filter in/3 ip destmask 255.0.0.0
set filter in/3 ip destaddr 211.0.0.0

// 禁止访问其他网站
// 新建 filter 策略 4（局部设置）
new filter in/4
set filter in/4 type ip
set filter in/4 forward no
// 设置要过滤的目的地址 0.0.0.0（通过 IP 地址和子网掩码定位需要过滤的 IP 地址段）
set filter in/4 ip destmask 0.0.0.0（0.0.0.0 代表任意网络掩码）
set filter in/4 ip destaddr 0.0.0.0（0.0.0.0 代表任意网络地址）

// 设置全局策略，允许其他所有数据包（必须有，且最后设置）
new filter in/5
set filter in/5 type generic
set filter in/5 forward yes

// 在 LAN 口上启用 Filter
set interface ethernet/1 ip filter enabled

// 保存上述配置
write

4.2 对源 IP 地址过滤

4.2.1 要求：允许内网某些用户访问 Internet，禁止其他所有用户访问 Internet

实例 3：

某局域网用的是 192.168.1.0/24 这个网段，先允许 192.168.1.1/24----192.168.1.31/24 上网，禁止其他 IP 地址的用户上网。

方法一：使用 IP Filter，利用 **Srcmask**[源 IP 掩码]和 **Srcaddr**[源 IP 地址]这两个参数，来定位需要过滤的 IP 地址段。

具体配置如下：

```
// 允许 IP 地址为 192.168.1.1/24----192.168.1.31/24 范围内的用户上网
// 新建 filter 策略 1（局部设置）
   new filter in/1
   set filter in/1 type ip
   set filter in/1 forward yes
// 设置要过滤的源网络的 IP 地址（通过 IP 地址和子网掩码定位需要过滤的 IP 地址段）
   set filter in/1 ip srcmask 255.255.255.224（利用 28 位的网络掩码来划分子网）
   set filter in/1 ip srcaddr 192.168.1.1（通过该网段中的任意一个地址来定义该网段）

// 禁止其他用户上网
// 新建 filter 策略 2（局部设置）
   new filter in/2
   set filter in/2 type ip
   set filter in/2 forward no
// 设置要过滤的源网络的 IP 地址（通过 IP 地址和子网掩码定位需要过滤的 IP 地址段）
   set filter in/2 ip srcmask 255.255.255.0
   set filter in/2 ip srcaddr 192.168.1.50

// 设置全局策略，允许其他所有数据包（必须有，且最后设置）
   new filter in/3
   set filter in/3 type generic
   set filter in/3 forward yes

// 在 LAN 口上启用 Filter
   set interface ethernet/1 ip filter enabled

// 保存上述配置
   write
```

方法二：使用 IPSSG Filter，利用 **SrcFrom**[源起始 IP 地址]和 **SrcEnd**[源结束 IP 地址]这两个参数，来定位需要过滤的 IP 地址段。

具体配置如下：

```
// 允许 IP 地址为 192.168.1.1/24----192.168.1.31/24 范围内的用户上网
```

// 新建 filter 策略 1（局部设置）
new filter in/1
set filter in/1 type ipssg
set filter in/1 forward yes
// 设置要过滤的源网络的 IP 地址（通过起始 IP 地址和结束 IP 地址定位需要过滤的地址段）
set filter in/1 ipssg srcfrom 192.168.1.1
set filter in/1 ipssg srcend 192.168.1.31

// 禁止其他用户上网，地址范围为 192.168.1.32/24----192.168.1.254/24
// 新建 filter 策略 2（局部设置）
new filter in/2
set filter in/2 type ipssg
set filter in/2 forward no
// 设置要过滤的源网络的 IP 地址（通过 IP 地址和子网掩码定位需要过滤的 IP 地址段）
set filter in/2 ipssg srcfrom 192.168.1.32
set filter in/2 ipssg srcend 192.168.1.254

// 设置全局策略，允许其他所有数据包（必须有，且最后设置）
new filter in/3
set filter in/3 type generic
set filter in/3 forward yes

// 在 LAN 接口上启用 Filter
set interface ethernet/1 ip filter enabled

// 保存上述配置
write

4.3 对局域网用户的服务过滤

4.3.1 要求 1：禁止在内网使用 MSN 聊天

实例 4：某公司希望禁止公司局域网用户使用 MSN 聊天。本例以 MSN6.2 为例说明，MSN 版本为 6.2 时，需要关闭 TCP 1863 和 TCP 443 两个端口。

具体配置如下：

// 禁止使用端口 1863
new filter in/1
set filter in/1 type IP
set filter in/1 forward no
set filter in/1 ip protocol 6
set filter in/1 ip destportcmp eql
set filter in/1 ip destport 1863

// 禁止使用端口 443
new filter in/2

```
set filter in/2 type IP
set filter in/2 forward no
set filter in/2 ip protocol 6
set filter in/2 ip destportcmp eql
set filter in/2 ip destport 443
```

// 设置全局策略，允许其他所有数据包（必须有，且最后设置）

```
new filter in/3
set filter in/3 type generic
set filter in/3 forward yes
```

// 在 LAN 口上启用 Filter

```
set interface ethernet/1 ip filter enabled
```

// 保存上述配置

```
write
```

4.3.2 要求 2：防冲击波/震荡波病毒

实例 5：冲击波/震荡波病毒是当前互联网中比较泛滥而且极度消耗网络资源的病毒，建议在 HiPER 中加以屏蔽。可通过关闭 TCP 135、137、139、445、1025、5554、9996 端口来实现。

具体配置如下：

// 关闭 TCP 135 端口

```
new filter in/1
set filter in/1 type ip
set filter in/1 forward no
set filter in/1 ip protocol 6
set filter in/1 ip destport 135
set filter in/1 ip destportcmp eql
```

// 关闭 TCP 137 端口

```
new filter in/2
set filter in/2 type ip
set filter in/2 forward no
set filter in/2 ip protocol 6
set filter in/2 ip destport 137
set filter in/2 ip destportcmp eql
```

// 关闭 TCP 139 端口

```
new filter in/3
set filter in/3 type ip
set filter in/3 forward no
set filter in/3 ip protocol 6
set filter in/3 ip destport 139
set filter in/3 ip destportcmp eql
```

```
// 关闭 TCP 445 端口
    new filter in/4
    set filter in/4 type ip
    set filter in/4 forward no
    set filter in/4 ip protocol 6
    set filter in/4 ip destport 445
    set filter in/4 ip destportcmp eql

// 关闭 TCP 1025 端口
    new filter in/5
    set filter in/5 type ip
    set filter in/5 forward no
    set filter in/5 ip protocol 6
    set filter in/5 ip destport 1025
    set filter in/5 ip destportcmp eql

// 关闭 TCP 5554 端口
    new filter in/6
    set filter in/6 type ip
    set filter in/6 forward no
    set filter in/6 ip protocol 6
    set filter in/6 ip destport 5554
    set filter in/6 ip destportcmp eql

// 关闭 TCP 9996 端口
    new filter in/7
    set filter in/7 type ip
    set filter in/7 forward no
    set filter in/7 ip protocol 6
    set filter in/7 ip destport 9996
    set filter in/7 ip destportcmp eql

// 设置策略，允许其他所有数据包（必须有，且最后设置）
    new filter in/8
    set filter in/8 type generic
    set filter in/8 forward yes

// 在 LAN 口上启用 Filter
    set interface ethernet/1 ip filter enabled

// 保存
    write
```

4.3.3 要求 3：禁止在内网使用 QQ 聊天

实例 6：某公司希望禁止公司局域网用户使用 QQ 聊天。本例中，QQ 版本号为：QQ2004 II 正式版 Build 12.73.8044。该版本 QQ 的服务器共有 18 个，地址如下：

61.144.238.146

61.144.238.145
61.141.194.203
219.133.38.5
219.133.38.43
219.133.38.44
219.133.38.45
219.133.38.47
219.133.38.141
219.133.38.230
219.133.40.215
219.133.40.216
202.104.129.251
202.104.129.252
202.104.129.253
202.104.129.254
218.18.95.153
218.17.209.23

可通过禁止内网用户访问这些服务器来实现，具体配置如下：

```
// 禁止内网用户访问指定服务器
new filter in/1
set filter in/1 type IP
set filter in/1 forward No
set filter in/1 ip destMask 255.255.255.255
set filter in/1 ip destAddr 61.144.238.145

new filter in/2
set filter in/2 type IP
set filter in/2 forward No
set filter in/2 ip destMask 255.255.255.255
set filter in/2 ip destAddr 61.144.238.146

new filter in/3
set filter in/3 type IP
set filter in/3 forward No
set filter in/3 ip destMask 255.255.255.255
set filter in/3 ip destAddr 61.141.194.203

new filter in/4
set filter in/4 type IP
set filter in/4 forward No
set filter in/4 ip destMask 255.255.255.255
set filter in/4 ip destAddr 219.133.38.43

new filter in/5
set filter in/5 type IP
set filter in/5 forward No
```

set filter in/5 ip destMask 255.255.255.255
set filter in/5 ip destAddr 219.133.38.44

new filter in/6
set filter in/6 type IP
set filter in/6 forward No
set filter in/6 ip destMask 255.255.255.255
set filter in/6 ip destAddr 219.133.38.45

new filter in/7
set filter in/7 type IP
set filter in/7 forward No
set filter in/7 ip destMask 255.255.255.255
set filter in/7 ip destAddr 219.133.38.47

new filter in/8
set filter in/8 type IP
set filter in/8 forward No
set filter in/8 ip destMask 255.255.255.255
set filter in/8 ip destAddr 219.133.40.215

new filter in/9
set filter in/9 type IP
set filter in/9 forward No
set filter in/9 ip destMask 255.255.255.255
set filter in/9 ip destAddr 219.133.40.216

new filter in/10
set filter in/10 type IP
set filter in/10 forward No
set filter in/10 ip destMask 255.255.255.255
set filter in/10 ip destAddr 202.104.129.251

new filter in/11
set filter in/11 type IP
set filter in/11 forward No
set filter in/11 ip destMask 255.255.255.255
set filter in/11 ip destAddr 202.104.129.252

new filter in/12
set filter in/12 type IP
set filter in/12 forward No
set filter in/12 ip destMask 255.255.255.255
set filter in/12 ip destAddr 202.104.129.253

new filter in/13
set filter in/13 type IP
set filter in/13 forward No

```
set filter in/13 ip destMask 255.255.255.255
set filter in/13 ip destAddr 202.104.129.254

new filter in/14
set filter in/14 type IP
set filter in/14 forward No
set filter in/14 ip destMask 255.255.255.255
set filter in/14 ip destAddr 219.133.38.5

new filter in/15
set filter in/15 type IP
set filter in/15 forward No
set filter in/15 ip destMask 255.255.255.255
set filter in/15 ip destAddr 219.133.38.141

new filter in/16
set filter in/16 type IP
set filter in/16 forward No
set filter in/16 ip destMask 255.255.255.255
set filter in/16 ip destAddr 218.18.95.153

new filter in/17
set filter in/17 type IP
set filter in/17 forward No
set filter in/17 ip destMask 255.255.255.255
set filter in/17 ip destAddr 219.133.38.230

new filter in/18
set filter in/18 type IP
set filter in/18 forward No
set filter in/18 ip destMask 255.255.255.255
set filter in/18 ip destAddr 218.17.209.23
// 设置全局策略，允许其他所有数据包（必须有，且最后设置）
new filter in/19
set filter in/19 type generic
set filter in/19 forward yes

// 在 LAN 口上启用 Filter
set interface ethernet/1 ip filter enabled

// 保存
write
```

4.4 配置基于时间的 Filter 策略

基于时间的 Filter 策略就是在配置的 Filter 策略中加入有效的时间范围来更合理有效的

控制网络。它需要先定义一个时间范围，然后在需要时间控制的 Filter 策略中应用它。需要注意的是，只有 IPSSG Filter 支持时间段控制，IP Filter 不支持。

4.4.1 要求：禁止内网某些用户在特定时间对 Internet 的访问

实例 7：在工作时间内，禁止 IP 地址为 192.168.1.114 的用户使用 FTP 传输文件，允许其他上网业务。在休息时间内，禁止该用户对 Internet 的所有访问。假设上述规定在 2005 年度有效，工作时间为：星期一～星期五，上午 09:00:00～11:59:59，下午 1:00:00～5:59:59；其余时间为休息时间。

分析：这里对时间段的配置进行简单分析。

根据该公司的规定，时间段生效的起始时间为 2005 年 1 月 1 日凌晨零点零分，结束时间为 2005 年 12 月 31 日 23:59:59

工作时间可以分为两个时间单元：

1. 星期一～星期五，09:00:00～11:59:59；
2. 星期一～星期五，13:00:00～17:59:59。

休息时间可以分为四个时间单元：

1. 星期一～星期五，00:00:00～08:59:59；
2. 星期一～星期五，12:00:00～12:59:59；
3. 星期一～星期五，18:00:00～23:59:59；
4. 星期六～星期天，00:00:00～23:59:59；

具体配置如下：

```
// 配置时间段 1——工作时间
// 该时间段名称定义为 worktime，在 2005 年度有效。
  new timerange/worktime
  set timerange/worktime Tmstart 2005-1-1    0:00:00
  set timerange/worktime Tmstop 2005-12-31 23:59:59
// 配置时间单元 1
  set timerange/worktime 1stperiod type weekday
  set timerange/worktime 1stperiod begin 09:00:00
  set timerange/worktime 1stperiod end 11:59:59
// 配置时间单元 2
  set timerange/worktime 2ndperiod type weekday
  set timerange/worktime 2ndperiod begin 13:00:00
  set timerange/worktime 2ndperiod end 17:59:59

// 配置时间段 2——休息时间
// 该时间段名称定义为 freetime，在 2005 年度有效。
  new timerange/freetime
  set timerange/freetimeTmstart 2005-1-1    0:00:00
  set timerange/freetime Tmstop 2005-12-31 23:59:59
// 配置时间单元 1
  set timerange/freetime 1stperiod type weekday
  set timerange/freetime 1stperiod begin 00:00:00
  set timerange/freetime 1stperiod end 08:59:59
```

// 配置时间单元 2
set timerange/freetime 2ndperiod type weekday
set timerange/freetime 2ndperiod begin 12:00:00
set timerange/freetime 2ndperiod end 12:59:59
// 配置时间单元 3
set timerange/freetime 3rdperiod type weekday
set timerange/freetime 3rdperiod begin 18:00:00
set timerange/freetime 3rdperiod end 23:59:59
// 配置时间单元 4
set timerange/freetime 4thperiod type weekend
set timerange/freetime 4thperiod begin 00:00:00
set timerange/freetime 4thdperiod end 23:59:59

// 工作时间内，禁止 IP 地址为 192.168.1.114 的用户使用 FTP 传输文件，即禁止该用户使用 FTP 端口（TCP:21）
new filter in/1
set filter in/1 type ipssg
set filter in/1 forward no
set filter in/1 ipssg timerange worktime（设置时间控制）
set filter in/1 ipssg srcmask 255.255.255.255
set filter in/1 ipssg srcaddr 192.168.1.114
set filter in/1 ipssg protocol 6
set filter in/1 ipssg destport 21
set filter in/1 ipssg destportcmp Eql

// 工作时间内，允许 IP 地址为 192.168.1.114 的用户所有其他上网业务
new filter in/2
set filter in/2 type ipssg
set filter in/2 forward yes
set filter in/2 ipssg timerange worktime（设置时间控制）
set filter in/2 ipssg srcmask 255.255.255.255
set filter in/2 ipssg srcaddr 192.168.1.114

// 休息时间内，禁止该用户对 Internet 的所有访问
new filter in/3
set filter in/3 type ipssg
set filter in/3 forward no
set filter in/3 ipssg timerange freetime（设置时间控制）
set filter in/3 ipssg srcmask 255.255.255.255
set filter in/3 ipssg srcaddr 192.168.1.114

// 设置全局策略，允许其他所有数据包（必须有，且最后设置）
new filter in/4
set filter in/4 type generic
set filter in/4 forward yes

// 在 LAN 口上启用 Filter

```
set interface ethernet/1 ip filter enabled
```

// 保存

```
write
```

附录一　常用 IP 协议号

协议	协议号	全称
IP	0	Internet Protocol
ICMP	1	Internet Protocol Message Protocol
IGMP	2	Internet Group Management
GGP	3	Gateway-Gateway Protocol
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Porotocl
PUP	12	PARC Universal Packet Protocol
UDP	17	User Datagram Protocl
HMP	20	Host Monitoring Protocol
XNS-IDP	22	Xerox NS IDP
RDP	27	Reliable Datagram Protocol
GRE	47	General Routing Encapsulation
ESP	50	Encap Security Payload
AH	51	Authentication Header
RVD	66	MIT Remote Virtual Disk
EIGRP	88	Enhandced Interior Gateway Routing Portocol
OSPF	89	Open Shortest Path First

附录二　常用 TCP/UDP 端口号

服务	端口号	协议	描述
echo	7	tcp	
echo	7	udp	
discard	9	tcp	
discard	9	udp	
systat	11	tcp	Active users
systat	11	udp	Active users
daytime	13	tcp	
daytime	13	udp	
qotd	17	tcp	Quote of the day
qotd	17	udp	Quote of the day
chargen	19	tcp	Character generator
chargen	19	udp	Character generator
ftp-data	20	tcp	FTP, data
ftp	21	tcp	FTP. control
telnet	23	tcp	
smtp	25	tcp	Simple Mail Transfer Protocol
time	37	tcp	timserver
time	37	udp	timserver
rlp	39	udp	Resource Location Protocol
nameserver	42	tcp	Host Name Server
nameserver	42	udp	Host Name Server
nicname	43	tcp	whois
domain	53	tcp	Domain Name Server
domain	53	udp	Domain Name Server
bootps	67	udp	Bootstrap Protocol Server
bootpc	68	udp	Bootstrap Protocol Client
tftp	69	udp	Trivial File Transfer
gopher	70	tcp	
finger	79	tcp	
http	80	tcp	World Wide Web
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
hostname	101	tcp	NIC Host Name Server
iso-tsap	102	tcp	ISO-TSAP Class 0
rtelnet	107	tcp	Remote Telnet Service
pop2	109	tcp	Post Office Protocol - Version 2
pop3	110	tcp	Post Office Protocol - Version 3

sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Identification Protocol
uucp-path	117	tcp	
nntp	119	tcp	Network News Transfer Protocol
ntp	123	udp	Network Time Protocol
epmap	135	tcp	DCE endpoint resolution
epmap	135	udp	DCE endpoint resolution
netbios-ns	137	tcp	NETBIOS Name Service
netbios-ns	137	udp	NETBIOS Name Service
netbios-dgm	138	udp	NETBIOS Datagram Service
netbios-ssn	139	tcp	NETBIOS Session Service
imap	143	tcp	Internet Message Access Protocol
pcmail-srv	158	tcp	PCMail Server
snmp	161	udp	
snmptrap	162	udp	SNMP trap
print-srv	170	tcp	Network PostScript
bgp	179	tcp	Border Gateway Protocol
irc	194	tcp	Internet Relay Chat Protocol
ipx	213	udp	IPX over IP
ldap	389	tcp	Lightweight Directory Access Protocol
https	443	tcp	MCom
https	443	udp	MCom
microsoft-ds	445	tcp	
microsoft-ds	445	udp	
kpasswd	464	tcp	Kerberos (v5)
kpasswd	464	udp	Kerberos (v5)
isakmp	500	udp	Internet Key Exchange
exec	512	tcp	Remote Process Execution
biff	512	udp	
login	513	tcp	Remote Login
who	513	udp	
cmd	514	tcp	
syslog	514	udp	
printer	515	tcp	
talk	517	udp	
ntalk	518	udp	
efs	520	tcp	Extended File Name Server
router	520	udp	route routed
timed	525	udp	
tempo	526	tcp	
courier	530	tcp	

conference	531	tcp	
netnews	532	tcp	
netwall	533	udp	For emergency broadcasts
uucp	540	tcp	
klogin	543	tcp	Kerberos login
kshell	544	tcp	Kerberos remote shell
new-rwho	550	udp	
remotefs	556	tcp	
rmonitor	560	udp	
monitor	561	udp	
ldaps	636	tcp	LDAP over TLS/SSL
doom	666	tcp	Doom Id Software
doom	666	udp	Doom Id Software
kerberos-adm	749	tcp	Kerberos administration
kerberos-adm	749	udp	Kerberos administration
kerberos-iv	750	udp	Kerberos version IV
kpop	1109	tcp	Kerberos POP
phone	1167	udp	Conference calling
ms-sql-s	1433	tcp	Microsoft-SQL-Server
ms-sql-s	1433	udp	Microsoft-SQL-Server
ms-sql-m	1434	tcp	Microsoft-SQL-Monitor
ms-sql-m	1434	udp	Microsoft-SQL-Monitor
wins	1512	tcp	Microsoft Windows Internet Name Service
wins	1512	udp	Microsoft Windows Internet Name Service
ingreslock	1524	tcp	
l2tp	1701	udp	Layer Two Tunneling Protocol
pptp	1723	tcp	Point-to-point tunnelling protocol
radius	1812	udp	RADIUS authentication protocol
radacct	1813	udp	RADIUS accounting protocol
nfsd	2049	udp	NFS server
knetd	2053	tcp	Kerberos de-multiplexor
man	9535	tcp	Remote Man Server